AO 106 (Rev. 04/10) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the

Northern District of Oklahoma

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

Hongjin Tan, 3312 Price Road, Apartment 5, Bartlesville, Oklahoma, 74006; A silver, 2013 Chevrolet Equinox, Oklahoma Tag EVY-204, registered to Hongjin Tan

Case No. 18-mj-175-JFJ

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):* Hongjin Tan, 3312 Price Road, Apartment 5, Bartlesville, Oklahoma, 74006; A silver, 2013 Chevrolet Equinox, Oklahoma Tag EVY-204, registered to Hongjin Tan

located in the Northern District of Oklahoma, there is now concealed *(identify the person or describe the property to be seized)*:
See Attached

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☑ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
Title 18, U.S.C. 1832(a)(2)	- Theft of Trade Secrets

The application is based on these facts:

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

James Clinton Judd, SA/FBI
Printed name and title

Sworn to before me and signed in my presence.

Date: 12-19-18

Judge's signature

City and state: Tulsa, OK

Magistrate Judge Jodi F. Jayne
Printed name and title

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

1. I am a Special Agent with the Federal Bureau of Investigation, and have been so employed since August of 1995. I am currently assigned to the Oklahoma City Division's Joint Terrorism Task Force, where I investigate multiple violations of Federal law, to include the investigation of economic espionage and theft of trade secrets. I have gained experience in conducting these investigations through training, seminars, and day-to-day work related to investigations of this type.

2. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

DESCRIPTION OF COMPANY A

3. Company A is a large international independent energy and petroleum corporation whose business focuses on exploration and development of petrochemical products and by-products and exploration and development of oil and natural gas. Company A's technology is critical to its business.

4. Company A protects its proprietary technology and processes through a multi-layered strategy involving both physical security as well as password protected entrance into varied computer systems.

COMPANY A'S PROPRIETARY TRADE SECRET INFORMATION RELEVANT TO THIS AFFIDAVIT

5. Company A has a research facility in Bartlesville, Oklahoma, with its headquarters in Houston, Texas. Company A sold and shipped, and intended to sell and ship, a product called "Premium Coke" which was developed and processed through Company A's proprietary process, in interstate and foreign commerce.

6. Company A manufactures gasoline and aviation fuel in Bartlesville, Oklahoma, and its Bartlesville facility is one of two refineries in the world to manufacture Premium Coke. Premium Coke is a product used in cell phone batteries, lithium car batteries, and graphite anodes (electrode through which current enters into a polarized electrical device – graphite is painted onto a copper surface which allows an oxidation reaction to occur).

7. Company A has advised the FBI that the company has earned an estimated $1.4 to $1.8 billion from its sale of Premium Coke. Company A considers its methods of developing Premium Coke to be trade secrets. The economic value of Company A's methods of developing Premium Coke is tremendously significant and of great value to competitors.

HONGJIN TAN

8. On 04/21/2017, Company A hired Hongjin Tan, a citizen of The People's Republic of China (now a Legal Permanent Resident of the United States), as a research engineer in the battery development group in Bartlesville, Oklahoma. Among other things, Tan was responsible for research and development of Company A's battery program operation, with the purpose of developing battery technology using Company A's proprietary processes.

9. In the resume Tan provided to Company A when he applied for employment, he listed his education as receiving a Bachelor of Science Degree in Physics from Nanjing University in Nanjing, China (2006), and he listed a Master's Degree and Doctorate Degree from the California Institute of Technology in Pasadena, California (2011).

COMPANY A CONTACT WITH THE FBI

10. On 12/13/2018, at approximately 12:19 p.m. Eastern Time, Micah Heilbrun, Special Counsel for Company A, called the FBI National Threat Operations Center (NTOC), formerly known as PAL, to report the theft of trade secrets. Heilbrun provided the below information.

11. On 12/12/2018 at approximately 10:30 a.m., Tan contacted his supervisor, Chris LaFrancois, and advised he was resigning from Company A and was serving notice of his two weeks before leaving Company A. Tan told LaFrancois that he was returning to China to be with his family as he is the only child to aging parents. Tan told LaFrancois that he did not currently have a job offer, but was negotiating with a few battery companies in China. As a result, LaFrancois informed his supervisor, Cathy Woody, of Tan's resignation.

12. Tan's resignation prompted Company A to revoke his access to company systems, and conduct a Systems Access review of Tan's computer activity. The review was conducted by Company A's Information Technology (IT) Librarian Laura Allen-Ward. Allen-Ward conducted the access review after learning of Tan's resignation/access deactivation.

13. On 12/12/2018 at around 3:30 pm, Allen-Ward notified Woody of unusual access research report access by Tan. The results of Tan's computer activity at Company A confirmed he had accessed hundreds of files, including research reports which, according to Company A, Tan had no business accessing. The reports included not only how to make Premium Coke, which, according to Company A, is a complicated and technically difficult process, but also Company A's plans for marketing Premium Coke in China and in cell phone and lithium-based battery systems. These files included information that Company A considers to be Trade Secrets.

14. Upon receiving this information from Allen-Ward, Woody determined Tan posed a potential high-risk to Company A by being capable of possessing and/or revealing

sensitive proprietary, trade-secret-protected information and decided to walk him out immediately.

15. At Woody's direction, LaFrancois located Tan and escorted him to LaFrancois' office, where they were met by Woody and Company A's Research and Development Shift Supervisor, Bryan Anderson. Woody told Tan he would not be allowed to come to Company A to finish his two weeks of notice employment and was to leave Company A's property immediately.

16. Woody permitted Tan to re-enter his office (CPL 218) to finish sending an email to Company A co-worker Neal McDaniel, after Woody reviewed the e-mail. Tan was also permitted to take his personal bag and keys home. Both of these items were searched by Woody and Anderson prior to Tan's exit from the site. Tan's personal bag was a laptop knapsack.

17. Later that day, on 12/12/2018 at approximately 4:00 p.m., Tan sent the following text message to Chris LaFrancois' cell phone:

"Hi Chris. This is Hongjin. Cathy was asking if there is anything I have with me associated with company IP. I have a memory disk that contains lab data that I plan to write report on, and papers/reports I plan to read at home. Now that I have been exited from (COMPANY A), can you check what is the best way of handling the information and how sensitive they are? Can I still read the papers/reports from the memory disk?"

18. In the above text message sent by Tan, Affiant believes his use of the letters "IP" referred to "Intellectual Property". Additionally, Affiant believes Tan confirmed he had data belonging to Company A at his home which he intended to write a report(s) about, despite the fact he had been barred from Company A's property.

19. After receiving the above text from Tan, LaFrancois asked Tan to return the flash drive (which Tan's text message referred to as a "memory disk") to Company A and informed Woody of Tan's requests.

20. At approximately 5:15 pm on 12/12/18, Tan returned to the Research Technology Center at Company A where he provided a USB flash drive to LaFrancois. The USB Flash Drive was Tan's personal property, which he was not authorized to utilize within Company A's space. There is no record of Company A having issued a USB Flash Drive to Tan.

21. After receiving the USB Flash Drive from Tan, LaFrancois immediately gave the USB flash drive to Company A's Director of IT Shared Services, Dennis Betterton. Company A believes that there was no break in chain of custody from LaFrancois to Betterton, who has maintained control of the flash drive to date.

EVALUATION OF POTENTIAL LOSS OF COMPANY A'S TRADE SECRET INFORMATION

22. Upon reviewing the USB Flash Drive, IT Director Betterton determined the following:

- the USB Flash Drive that was in Tan's possession outside of Company A's control contained data files that were owned solely by Company A, and;

- data on the USB Flash Drive that was in Tan's possession (in deleted and undeleted files) contained research documents which would have a tremendous impact to Company A in terms of technological and economic loss if they were to be shared or given to a competing company. Each page of the accessed document(s) was marked "confidential" and "restricted".

23. During Betterton's review, he determined the files which were deleted from the USB Flash Drive, were deleted on 12/11/2018, the day before Tan's resignation. Those deleted files remained on the flash drive in unallocated space. Company A reviewed the deleted files (in addition to files on the USB Flash Drive), and conducted a Risk Assessment for the data. Company A's Risk Assessment included assigning the files "Technology Accessed Risk Levels." Data found on the USB Flash Drive given to Company A by Tan included documents that Company A assigned Technological Accessed Risk Levels ranging from Low-Medium to Extremely High.

24. A portion of the Risk Assessment Summary and comments are as follows:

DOCUMENT ID	SUMMARY OF RISK ITEM	POTENTIAL HARM TO COMPANY A	TECHNOLOGY ACCESSED RISK LEVEL
204488297	Highly sensitive document that details process to formulate premium coke technology from (Company A's Refineries). This technology cannot be utilized in every refinery but discloses all of Company A's optimizations and operating ranges necessary to make premium coke.	Full erosion of (Company A's) premium coke business. If disclosed outside (Company A), competitors with refinery specifications could replicate (Company A's) premium coke.	Extremely High
228709681	Document details how (Company A's) premium coke users could utilize the starting materials of (Company A's) premium coke to make their own premium coke. If disclosed outside (Company A), this document will erode (Company	Partial erosion of (Company A's) premium coke business. If (Company A's) customers gained access to this information, it would allow them to manufacture their own premium coke	High

	A's) pricing and market share in the premium coke business		

25. On 12/14/2018, Company A Special Counsel Heilbrun told Affiant that IT specialists for Company A were able to ascertain Tan accessed Company A data over the period of the last month, which Tan had no reason or authority to access. According to Company A IT Specialists, Tan downloaded hundreds of files to multiple thumb drives or other removable media. Tan did not report this access and was not granted authority by Company A to download or remove this data from Company A. Tan turned in one USB flashdrive but did not turn in any other removable media onto which he downloaded proprietary information belong to Company A. This was determined from Company A's basic analysis assessment using commercially available computer forensic software. In addition, on the one USB Flash Drive Tan did return to Company A, Tan had downloaded trade secrets and then deleted those trade secrets prior to returning the Flash Drive to Company A. Affiant believes Tan maintained possession of additional drives or other removable media which contain trade secrets owned by Company A.

DESCRIPTION OF TAN'S CONTACT WITH COMPETITOR OF COMPANY A

26. On 12/13/2018, Tan had dinner with his former co-worker at Company A, Neal McDaniel. During this dinner, Tan told McDaniel he was leaving Oklahoma on 12/27/2018 to return to China. Tan told McDaniel that when he went to China in September 2018, he interviewed for a Chinese company named Xiamen Tungsten Corporation and had been in constant contact with the company since he was in graduate school at The California Institute of Technology.

27. The following day (12/14/2018), McDaniel reported the conversation he had with Tan at dinner to Cathy Woody.

28. According to the website for Xiamen Tungsten Corporation (www.cxtc.com), the company is located in Xiamen, China. According to the online company profile (which is available in Chinese and English) for Xiamen Tungsten, the company has "developed two production lines so far, one for Li-ion battery cathode materials (such as lithium cobalt oxide, ternary cathode material, lithium manganese oxide, lithium iron phosphate, etc.) and the other for NiMH battery anode material (Hydrogen storage alloy)."

29. Upon reading the company profile for Xiamen Tungsten, Affiant believes the Xiamen Tungsten Company could be considered a competitor of Company A's in the area of battery development and technology.

TAN'S FOREIGN TRAVEL

30. Affiant has located international travel records for Tan from the United States (U.S.) Customs and Border Protection and U.S. Department of Homeland Security. These records confirm that on 09/15/2018, Tan traveled from the Dallas/Ft. Worth, Texas

International Airport to Peking, China and arrived at the Beijing, China Capital International Airport. Tan's travel records also confirm that on 09/30/2018, he returned to the Dallas/Ft. Worth, Texas International Airport via the Beijing, China Capital International Airport.

COMPANY A'S PROTECTION OF ITS TRADE SECRETS

31. Company A's methods of developing premium coke were protected by Company A as confidential and proprietary information. Company A considers this information to be a trade secret (hereinafter referred to as the Trade Secret Information), which was used in products sold and distributed in interstate or foreign commerce.

32. Company A used a number of reasonable measures to protect the Trade Secret Information and its other confidential proprietary information, including the following:

- Company A restricted access to the controlled environment in Oklahoma where the premium coke and battery research were conducted behind locked doors with magnetic card readers, and only certain employees were granted access;

- Company A limited access to the Trade Secret Information to those who needed it to perform their employment duties;

- Company A prohibited distribution of research products to other companies, persons, or countries or for research;

- as a condition of their employment, Company A employees executed non-disclosure and assignment agreements, which specifically referenced Company A's confidential and proprietary information.

33. Company A implemented data security policies stipulating that all information created, sent, received, or stored on Company A's electronic resources was company property and that all activity on Company A's electronic resources was subject to monitoring. Furthermore, these policies prohibited employees from transmitting, receiving, or storing company information outside Company A's electronic resources.

34. Affiant believes Tan was aware of Company A's measures to protect their Trade Secret Information due to the agreements he signed with Company A pertaining to Confidential Information, Non-Disclosure and Intellectual Property.

35. As an example, in the Confidential Information, Non-Disclosure and Intellectual Property Agreement signed by Tan on 06/19/2018, Tan agreed, among other things, that;

- without prior written consent of Company A, he would not "disclose, use, reproduce, or transmit (except for the performance of his duties for Company A), or permit the unauthorized disclosure, use, reproduction or transmission of any Confidential

Information during the period of his employment with Company A or at any time thereafter";

- he would not "upon leaving the employ" of Company A (Tan's resignation was accepted and in effect immediately upon serving it on 12/12/2018), take with him any records, memoranda, drawings, pictures, models, papers, notebooks, reports, computer disks or other similar media having Confidential Information in or on such media.

36. Additionally, Affiant believes Tan was reminded of his obligation, per signed agreement, with Company A when he would log in to his work computer.

37. For example, when an employee of Company A begins to access their computer at work, the following warning appears on a screen banner before the employee can log in:

"This is a private computer system to be accessed and used for (Company A) business purposes. By accessing, using and continuing to use this system or device, you agree to the terms of use. All access must be specifically authorized and used only in accordance with all applicable (Company A) policies. Unauthorized access or use of this system is prohibited and may expose you to liability under criminal and civil laws. Absent a separate written agreement, all non-personal information and content you create, store or collect on behalf of (Company A) or in the scope of your employment, on this computer system is the sole property of (Company A). To the extent permitted under local law, (Company A) reserves the right to monitor, access, intercept, records, read, copy, capture and disclose all information received, sent through or stored in this system or device, without notice, for any purpose and at any time."

38. After the Company A employee successfully logs into Company A's computer systems, the exact same warning appears on the computer screen under the heading "**LEGAL NOTICE**".

39. Additionally, according to Company A's Special Counsel Heilbrun, the wording in a warning window described below appears anytime a Company A employee activates Company A's Virtual Private Network (VPN), which is a process which allows an employee to access Company A's computer systems remotely:

"When logging into (Company A's) network(s) you agree to comply with all applicable export control regulations. Further you agree you will not access (Company A's) network from any countries subject to comprehensive U.S. Embargoes/Sanctions, including Cuba, Iran, North Korea, Sudan, or Syria."

40. Heilbrun also advised it is not possible to successfully activate Company A's VPN without seeing the above described three warning banners.

41. Company A provided Tan's address to Affiant as 3312 Price Road, Apartment 5, Bartlesville, Oklahoma.

42. On 12/16/2018 at approximately 13:30 p.m., FBI Special Agent Ashley Dublin observed Tan driving a silver, 2013 Chevrolet Equinox bearing Oklahoma License Plate EVY-024 to a restaurant in Bartlesville, Oklahoma from his residence at 3312 Price Road, Apartment 5, Bartlesville, Oklahoma. According to employees at Company A, this is the vehicle Tan routinely drove to his place of employment.

43. Affiant has obtained the registration for this vehicle from the Oklahoma Tax Commission (OTC). OTC records confirm the vehicle bearing Oklahoma License Plate EVY-024 is registered to Hongjun, Tan at 3312 Price Road, Apartment 5, Bartlesville, Oklahoma.

For the reasons stated above, Affiant submits there is probable cause to believe that Tan's residence (described in Attachment A) and vehicle (described in Attachment B) contain evidence of a crime; contraband, fruits of crime, or other items illegally possessed; and property designed for use, intended for use, or used in committing a crime; those crimes being violations of 18 U.S.C. § 1832(a) (Theft of Trade Secrets). Such items include documents representing Trade Secret Information and proprietary Information owned by and belonging solely to Company A, which is stored in and on computer equipment, media, files and other formats (described in Attachment C), and any related information in any form, such as hard copy formats such as print-outs, copies, or original paper documents.

Respectfully submitted,

James Clinton Judd
Special Agent FBI

Subscribed and sworn to before me this 19th day of December 2018.

Honorable Jodi F. Jayne
United States Magistrate Judge

Attachment "A"

Property to be searched

The premises to be searched is 3312 Price Road, Apartment 5, Bartlesville, Oklahoma 74006. The property to be searched is described as a two-story, attached apartment composed of a brick exterior with a black shingle roof and exterior window on the second floor surrounded by tan siding. The apartment has two windows on the first floor exterior trimmed in white. The front door of the apartment is white in color with a paned window set in the door and the number "5" set to the right of the door.

Attachment "B"

Property to be searched

The vehicle to be searched is a white, 2013 Chevrolet Equinox, Oklahoma Tag EVY-024, registered to a Hongjin Tan, 3312 Price Road, Apartment 5, Bartlesville, Oklahoma 74006. The vehicle is further described as a white, four door sports utility vehicle with a round, California Institute of Technology sticker in the rear window, and registration sticker number of U392367 on the license plate.

Attachment "C"

Property to be seized

1. All records relating to violations of 18 U.S.C. Section 1832(a)(2), those violations involving Hongjin Tan and occurring after April 21, 2017, including:

a. Records and information relating to a conspiracy to defraud Company A as referenced in the affidavit;

b. Records and information relating to an access of Company A computers;

c. Records and information relating to Company A;

d. Records and information relating to Tan's e-mail accounts;

e. Records and information relating to the identity or location of the suspects;

f. Records and information relating to trade secrets, protected or confidential information owned by Company A;

g. Records maintained on cell phone(s) on the premises of to be searched.

2. Computers or storage media used as a means to commit the violations described above, including downloading confidential materials without authorization in violation of 18 U.S.C. § 1832(a)(2).

3. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):

a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

c. evidence of the lack of such malicious software;

d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;

e. evidence indicating the computer user's state of mind as it relates to the crime under investigation;

f. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

g. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;

h. evidence of the times the COMPUTER was used;

i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

k. records of or information about Internet Protocol addresses used by the COMPUTER;

l. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;

m. contextual information necessary to understand the evidence described in this attachment.

4. Routers, modems, and network equipment used to connect computers to the Internet.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions,

including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.